



FAQs on CSCRf Policies templates provided by APMI

1. What are Cyber Security Policies under the CSCRf framework?

- a. As per SEBI's circular dated August 20, 2024, regulated entities (REs) are required to adopt specific Cyber Security Policies, based on their categorization.
- b. These policies form the backbone of the Cyber Security and Critical Resilience Framework (CSCRf), aiming to protect critical information infrastructure, ensure operational resilience, and maintain regulatory compliance.
- c. The set of policies adopted in line with this framework is collectively referred to as **CSCRf Policies**.

2. What initiative has APMI taken to support compliance with the CSCRf framework?

- a. APMI has taken the below 4 key initiatives towards simplifying CSCRf compliance for its members:
 - 1. SOC Services:**
 - 2. VAPT Service:**
 - APMI has secured composite & discounted price quotation for M-SOC and VAPT services from BSE M-SOC- BluSapphire Cyber Systems Pvt. Ltd. for its members.
 - The same was communicated to the APMI members vide email dated March 17, 2025.
 - 3. CSCRf Policy Templates:**
 - APMI, in collaboration with Elytra Security Private Limited, has developed a standardized set of Cyber Security policy templates tailored for self-certified and mid-sized regulated entities.
 - To facilitate better understanding, APMI is conducting two Compliance Sutra sessions in April 2025 with Elytra Security, dedicated to explaining these templates.
 - 4. Cyber Training:**
 - This is currently under discussion at the Board level, and we will update you shortly on this.

3. Who is Elytra Security Private Limited & why has APMI chosen them?

- a. Elytra Security is a specialized information security advisory and consulting firm dedicated to helping organizations fortify their information security and achieve compliance with globally recognized standards.
- b. With expertise in ISO 27001 implementation and SEBI's Cyber Security and Cyber Resilience Framework (CSCRf) consulting, they deliver tailored solutions that empower businesses to protect sensitive information, mitigate risks, and demonstrate robust security practices.
- c. APMI had invited proposals and quotations from a group of Cyber Consultants and based on the service offered, quotation received and in line with the approval from the APMI Board, we chose Elytra Security Private Limited for this initiative.



4. How many policy templates are provided under this initiative?

- a. A total of **14 policy templates** are being made available to the APMI members.
- b. These are standard reference documents, and Portfolio Managers may customize them to align with their specific IT infrastructure and operational requirements.

5. Where can APMI Members access the CSCRf policy templates?

- a. APMI Members can access the templates through their APMI login by following this path- [APMI Member Login](#) > [CSCRf Policy Templates](#) > [Accept the Terms & Conditions](#) > [Download the Zip folder](#).
 - i. Which has **14-word files (Policy Templates)** & **1 PDF doc (Control Document)**.

6. Is it mandatory for PMS entities to adopt these policy templates?

- a. The templates provided by APMI are **purely supportive in nature** and are **not mandatory**.
- b. PMS entities are free to design, implement & execute their own cybersecurity policies, as deemed appropriate.

7. What is the 'Legend Table' found at the end of each policy template?

- a. Each policy template concludes with a legend table, which uses a color-coded format to provide guidance:
 - i. **Grey denoting**- Mandatory requirements for Mid-sized RE's.
 - ii. **Yellow denoting**- Elements to be customized as per the organization's context.
 - iii. **Green denoting**- Timeframes or frequency of actions.

8. What is being referred to as the 'Control Document'?

- a. The control document is a supporting guide that maps each policy template to the relevant CSCRf requirements.
- b. It also outlines the applicability of each policy to different categories of regulated entities.

9. How do the CSCRf policy templates apply across different RE categories?

- a. This has been clarified in the control document:
 - i. **Mid-sized REs**: All 14 policy templates are applicable.
 - ii. **Self-certified REs**: 12 out of 14 policy templates are mandatory. Two (2) policy templates, **Risk Management** and **Business Continuity & Disaster Recovery**, are optional but encouraged.

10. What aspects are outside APMI's scope regarding these policies & templates provided?

- a. APMI's role is limited to providing standardized policy templates.
- b. The implementation & execution of these policies is the sole responsibility of the respective PMS.
- c. Customizations specific to individual entities are beyond APMI's scope.



- d. Any engagement between APMI Members and Elytra Securities is outside the ambit of APMI.
- e. APMI will **not**:
 - i. Conduct security solution reviews, Vulnerability Assessment and Penetration Testing (VAPT), code reviews, or configuration security reviews.
 - ii. Update security policies or processes.
 - iii. Prepare regulatory reports or provide legal advice or reviews.
 - iv. Develop or implement device-level or other technical documentation.
 - v. Provide or issue any certification for regulatory compliance as part of this initiative.

For any further clarifications, members are requested to submit their queries exclusively through the **Query Management tab** available in their member login portal.

-----**END OF THE DOCUMENT**-----